与SPA2102、SPA3102和SPA9000的基于HTTPS的远程供应

目录

简介

本文是一系列协助设置、排错和维护Cisco小型企业产品(以前Linksys企业系列)文档中的一篇。

Q. 使用SPA2102、SPA3102和SPA9000，我无法验证到HTTPS服务器。问题出在哪里？

A.

在一些SPA2102、SPA3102和SPA9000设备的客户端证书被制造在**十一月15， 2005年**和**六月15之间， 2006**不正确地安装。此缺陷影响HTTPS提供的功能。

有不正确证书的设备将发生故障***客户端验证***用HTTPS服务器。

此缺陷，然而，不影响设备的适当的功能，包括HTTPS服务器验证，所有电话作用，远程固件升级和TFTP和HTTP基于供应。安全供应可以通过传送已加密供应文件执行通过TFTP或HTTP。已加密语音功能也没有受影响。

某些，但是不是所有，在以下范围的设备序列号有不正确客户端证书：

产品	范围序列号
SPA2102	FM500F100000 - FM500F699999
??SPA3102	??FM600F100000 - FM600F699999
SPA9000	FM700F100000 - FM700F699999

如果您的设备有此缺点，并且设备需要远程设置，您可以采取以下行动之一：

以已加密供应配置文件使用HTTP或TFTP基于供应。
使用HTTPS供应以：
启用的服务器验证，
禁用的客户端验证或者
已加密供应配置文件(加密通过Linksys SPC工具或openssl)。

有正确地安装的客户端证书的设备是现在可以得到的。

相关信息

- 技术支持&文档- Cisco系统。